What is claimed is:

Sub a19

1.   A computerized wagering game apparatus, comprising:

a computerized game controller having a processor, memory, and nonvolatile storage and operable to control the computerized wagering game; and

5   game data stored in the nonvolatile storage, wherein the game data stored in nonvolatile storage is verified during operation.

2.   The computerized wagering game apparatus of claim 1, wherein the game data securely stored in the nonvolatile storage is hashed with a one-way hash function

10   and a resulting hash value is compared to a reference hash value to ensure that the gaming program has not changed since calculation of the reference hash value.

3.   The computerized wagering apparatus of claim 2, wherein the game data is hashed after loading the gaming program into random access memory and the resulting

15   hash value is compared to a reference hash value in a continuously executing program thread executing on the computerized game controller.

4.   The computerized wagering game apparatus of claim 2, wherein the computerized wagering game system is brought to a tilt state if the resulting hash value is

20   not the same as the reference hash value.

5.   The computerized wagering game apparatus of claim 2, wherein the reference hash value is stored in a nonvolatile memory comprising a part of the computerized wagering game apparatus.

25

6.   The computerized wagering game system of claim 1, wherein a system handler application loads and executes encryption functions which are subsequently used to securely load other game data from nonvolatile storage.

20

7. The computerized wagering game apparatus of claim 1, wherein the game data securely stored in the nonvolatile storage via encryption is signed with a digital signature.

5　　8. The computerized wagering game apparatus of claim 7, wherein the digital signature comprises encryption of the gaming program data with a signer's private key.

9. The computerized wagering game apparatus of claim 8, further comprising 10　a nonvolatile memory storing a public key corresponding to the signer's private key.

10. The computerized wagering game apparatus of claim 7, wherein the digital signature comprises encryption with a signer's private key of a hash value produced by hashing the gaming program data with a one-way hash function.

15

11. The computerized wagering game apparatus of claim 10, further comprising a nonvolatile memory storing a public key corresponding to the signer's private key.

20　　12. The computerized wagering game apparatus of claim 7, wherein the gaming program data signed with a digital signature is signed with a digital signature from a regulatory organization, thereby signifying organization approval of the gaming program data.

25　　13. The computerized wagering game apparatus of claim 1, wherein the computerized game controller is a general-purpose computer.

14. The computerized wagering game apparatus of claim 12, wherein the general-purpose computer is an IBM PC-compatible computer.

15.   The computerized wagering game apparatus of claim 1, further comprising a network interface connecting the computerized wagering game apparatus to a networked computer.

5   16.   A method for securing data on a computerized wagering game apparatus, comprising verification of game data located in RAM during operation of a computerized gaming apparatus.

17.   The method of claim 16, further comprising encryption of data

10   communicated via the computerized wagering game apparatus over a network.

18.   The method of claim 17, wherein the data communicated over the network comprises instructions to control the operation of the computerized wagering game.

15   19.   The method of claim 17, wherein the data communicated over the network comprises shared objects for execution on the computerized wagering game.

20.   The method of claim 17, wherein the data communicated over the network comprises data reported by the computerized wagering game.

20

21.   The method of claim 16, wherein encryption of data stored in the computerized gaming apparatus comprises:

    hashing the stored data with a one-way hash function; and

    comparing a resulting hash value to a reference hash value to ensure that the data

25   has not changed since calculation of the reference hash value.

22.   The method of claim 21, wherein the reference hash value is stored in nonvolatile memory that comprises a part of the computerized wagering game apparatus.

23. The method of claim 16, wherein hashing the stored data with a one-way hash function comprises:

loading the data into random access memory;

hashing the stored data with a one-way hash function in a continuously executing

5   thread; and

comparing a resulting hash value to a reference hash value in a continuously

executing thread to ensure that the data has not changed since calculation of the reference

hash value.

10   24. The method of claim 21, further comprising bringing the computerized

wagering game to a tilt state if the resulting hash value is not the same as the reference

hash value.

25. The method of claim 16, wherein encryption of data stored in the -

15   computerized gaming apparatus comprises signing the data with a digital signature.

26. The method of claim 25, wherein signing the data with a digital signature

comprises encryption of the data with a signer's private key.

20   27. The method of claim 26, wherein a public key corresponding to the

signer's private key is stored in nonvolatile memory comprising a part of the

computerized wagering game apparatus.

28. The method of claim 26, wherein signing the data with a digital signature

25   comprises:

computing a hash value from the data produced with a one-way hash function;

and

encrypting the hash value with a signer's private key.

29. The method of claim 28, wherein a public key corresponding to the signer's private key is stored in nonvolatile memory comprising a part of the computerized wagering game apparatus.

5   30. The method of claim 16, wherein the computerized wagering game apparatus comprises a general-purpose computer.

31. The method of claim 30, wherein the general-purpose computer comprises an IBM PC-compatible computer.

10

32. The method of claim 16, wherein encrypting data comprises use of a symmetric encryption algorithm to encrypt data.

33. A machine-readable medium with instructions stored thereon, the
15   instructions when executed operable to cause a computerized wagering game apparatus to:

   apply encryption to data stored in the computerized gaming apparatus.

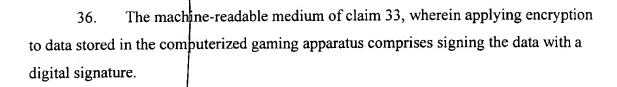34. The machine-readable medium of claim 33, further comprising
20   instructions that when executed are further operable to cause the computerized wagering game apparatus to:

   apply encryption to data communicated via the computerized wagering game apparatus over a network.

25   35. The machine-readable medium of claim 33, wherein applying encryption to data stored in the computerized gaming apparatus comprises:

   hashing the data with a one-way hash function; and

   comparing a resulting hash value to a reference hash value to ensure that the data has not changed since calculation of the reference value.

24

36.   The machine-readable medium of claim 33, wherein applying encryption to data stored in the computerized gaming apparatus comprises signing the data with a digital signature.

5   37.   The machine-readable medium of claim 36, wherein signing the data with a digital signature comprises encryption of the data with a user's private key.

38.   The machine-readable medium of claim 36, wherein signing the data with a digital signature comprises:

10   computing a hash value from the data produced with a one-way hash function; and

encrypting the hash value with a signer's private key.

39.   A computerized wagering game apparatus, comprising:

15   a computerized game controller having a processor, memory and nonvolatile storage and operable to control the computerized wagering game;

gaming program code and gaming program code signature stored in the nonvolatile storage, and

an authentication program stored in nonvolatile storage, wherein the

20   authentication program, when executed, verifies that the gaming program code in nonvolatile storage has not changed by means of generating a message digest from the gaming program code, decrypting the message digest using a first decryption program; decrypting the gaming program code signature with a second decryption program and comparing the two decrypted messages to verify that they are identical.

25